CREDIT REPORT AUTHORIZATION AND RELEASE

Authorization is hereby granted to _____ (Company) to obtain a standard factual data credit report through a consumer credit reporting agency chosen by Company.

_____ _____

Social Security Number Date of Birth

_____ _____ _____

Last Name First Name M.I.

_____

Street

_____ _____ _____

City State Zip Code

_____

Phone Number

_____ _____

Signature Date

Red Flag

FTC FACTS for Business

FEDERAL TRADE COMMISSION 1-877-FTC-HELP FOR THE CONSUMER FTC.GOV

Information Compromise and the Risk of Identity Theft: Guidance for Your Business

These days, it is almost impossible to be in business and not collect or hold personally identifying information — names and addresses, Social Security numbers, credit card numbers, or other account numbers — about your customers, employees, business partners, students, or patients. If this information falls into the wrong hands, it could put these individuals at risk for identity theft.

Still, not all personal information compromises result in identity theft, and the type of personal information compromised can significantly affect the degree of potential damage. What steps should you take and whom should you contact if personal information is compromised? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC), the nation's consumer protection agency, can help you make smart, sound decisions.

Check federal and state laws or regulations for any specific requirements for your business.

Notifying Law Enforcement

When the compromise could result in harm to a person or business, call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service. Check the blue pages of your telephone directory or an online search engine for the number of the nearest field office.

Notifying Affected Businesses

Information compromises can have an impact on businesses other than yours, such as banks or credit issuers. If account access information — say, credit card or bank account numbers — has been stolen from you, but you do not maintain the accounts, notify the institution that does so that it can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other businesses, notify them of any information compromise, as well.

If names and Social Security numbers have been stolen, you can contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts for their files. Your notice to the credit bureaus can facilitate customer assistance.

Equifax
U.S. Customer Services
Equifax Information Services, LLC
Phone: 1-800-685-1111
Email:
businessrecordsecurity@equifax.com

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Email:
BusinessRecordsVictimAssistance@experian.com

TransUnion
Phone: 1-800-372-8391

If the information compromise resulted from the improper posting of personal information on your website, immediately remove the information from your site. Be aware that Internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure that they do not archive personal information that was posted in error.

Notifying Individuals

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Social Security numbers can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take some steps to prevent or limit any harm.

When notifying individuals, the FTC recommends that you:

- consult with your law enforcement contact about the timing of the notification so it does not impede the investigation.
- designate a contact person within your organization for releasing information. Give the contact person the latest information about the breach, your response, and how individuals should respond. Consider using letters (see sample on page 4), websites, and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your notice:

- describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation.
- explains what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports.

See www.ftc.gov/idtheft for more complete information on appropriate follow-up after a compromise.

- includes current information about identity theft. The FTC's website at www.ftc.gov/idtheft has information to help individuals guard against and deal with identity theft.
- provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.
- encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

Model Letter

The letter on page 4 is a model for notifying people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

For More Information

This publication provides general guidance for an organization that has experienced an information compromise. If you would like more individualized guidance, you may contact the FTC at idt-brt@ftc.gov. Please provide information regarding what has occurred, including the type of information taken, the number of people potentially affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national victim complaint database, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, if you prefer to seek guidance anonymously, you may do so.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

FTC FACTS for Business

ftc.gov
For The Consumer
Federal Trade Commission
1-877-FTC-HELP

Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft

The Fair Credit Reporting Act (FCRA) spells out rights for victims of identity theft, as well as responsibilities for businesses. Identity theft victims are entitled to ask businesses for a copy of transaction records — such as applications for credit — relating to the theft of their identity.

Indeed, victims can authorize law enforcement officers to get the records or ask that the business send a copy of the records directly to a law enforcement officer. The businesses covered by the law must provide copies of these records, free of charge, within 30 days of receiving the request for them in writing. This means that the law enforcement officials who ask for these records in writing may get them from your business without a subpoena, as long as they have the victim's authorization.

The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the FCRA including this requirement, which is known as Section 609(e). Here is some additional information to help your business comply with this provision of the law:

Q. Who must comply with Section 609(e) of the FCRA?

A. The law applies to a business that has provided credit, goods, or services to, accepted payment from, or otherwise entered into a transaction with someone who is believed to have fraudulently used another person's identification. For example, if your business opened a cell phone account in the victim's name or extended credit to someone misusing the victim's identity, you may be required to provide the records relating to the transaction to the identity theft victim or the law enforcement officer acting on that victim's behalf.

Q. What documents must my business provide?

A. Your business must provide applications and business transactions records, maintained either by your business or by another entity on your behalf, that support any transaction alleged to be a result of identity theft. Records like invoices, credit applications, or account statements may help victims document the fraudulent transaction and provide useful evidence about the identity thief.

Q. What are the procedures for requesting these materials?

A. Requests for documents must be submitted in writing. Your business may specify an address to receive these requests. You may ask the victim to provide relevant information, like the transaction date or account number, if they know it. You also can require that victims provide:

1. proof of identity, like a government-issued ID card, the same type of information the identity thief used to open the account, or the type of information you are currently requesting from applicants; and
2. a police report and completed affidavit. Victims can use the FTC's ID Theft Affidavit, available at ftc.gov/idtheft, or another affidavit you accept.

Q. Is it ever appropriate not to provide documents?

A. You can refuse to provide the records if you determine in good faith that:

- you cannot verify the true identity of the person asking for the information;
- the request for the information is based on a misrepresentation; or
- the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

Your business may not deny disclosure of these records based on the financial privacy provisions of the Gramm-Leach-Bliley Act (see Subtitle A of Title V of Public Law 106-102). Nevertheless, you may refuse to disclose them if state or another federal law prohibits you from doing so.

Q. Are there recordkeeping requirements of Section 609(e)?

A. Section 609(e) does not require any new recordkeeping procedures for your business.

For More Information

The FTC works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help businesses comply with a wide variety of rules and regulations. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. To file an identity theft complaint and obtain more information about how to minimize your risk and remedy the effects of identity theft, visit ftc.gov/idtheft or call the toll-free hotline at 1-877-ID-THEFT (1-877-438-4338). The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to over 1400 civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

May 2006

FTC Consumer Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Office of Consumer & Business Education

How Not to Get Hooked by a 'Phishing' Scam

"We suspect an unauthorized transaction on your account.
To ensure that your account is not compromised,
please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information.
Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.** Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.

- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.

- **Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

  Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

  A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- **Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

- **Forward spam that is phishing for information** to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

- **If you believe you've been scammed, file your complaint at ftc.gov**, and then visit the FTC's Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

  You can learn other ways to avoid email scams and deal with deceptive spam at ftc.gov/spam.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them.

To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

October 2006

To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

October 2006

Identify Theft Victims Statement of Rights

Several federal laws protect victims of identity theft. These laws have to do with documenting the theft; dealing with credit reporting companies; dealing with creditors, debt collectors, and merchants; and limiting your financial losses caused by the theft of your identity. Here is a brief summary of the rights of identity theft victims, with links to websites that provide more information.

Documenting the Theft

You have the right to:

- File a report with a law enforcement agency and ask for a copy of it to show how your identity has been misused. This report is often called a police report.

An identity theft report is a second kind of report. It is a police report with more detail. To be an identity theft report, it should have enough information about the crime that the credit reporting companies and the businesses involved can verify that you're a victim, and know which accounts or information have been affected. It's the report that will give you access to many of the rights described here.

The FTC's ID theft complaint form is a good place to start documenting the theft of your identity. This form asks you for the kind of detail that the identity theft report requires. Once you fill out this form online and print it, you can use it with the police report to create your identity theft report.

Dealing with Credit Reporting Companies

You have the right to:

- Place a 90-day initial fraud alert on your credit files. You would do this if you think you are — or may become — the victim of identity theft. A fraud alert tells users of your credit report that they must take reasonable steps to verify who is applying for credit in your name. To place a 90-day fraud alert, contact just one of the three nationwide credit reporting companies. The one you contact has to notify the other two.
- Place a seven-year extended fraud alert on your credit files. You would do this if you know you are a victim of identity theft. You will need to give an identity theft report to each of the credit reporting companies. Each credit reporting company will ask you to give them some way for potential creditors to reach you, like a phone number. They will place this contact information on the extended fraud alert as a signal to those who use your credit report that they must contact you before they can issue credit in your name.
- Get one free copy of your credit report and a summary of your rights from each credit reporting company. You can get these when you place a 90-day initial fraud alert on your credit reports. When you place an extended fraud alert with any credit reporting company, you have the right to two copies of that credit report during a 12-month period. These credit reports are in addition to the free credit report that all consumers are entitled to each year.

- Ask the credit reporting companies to block fraudulent information from appearing on your credit report. To do this, you must submit a copy of a valid identity theft report. The credit reporting companies then must tell any creditors who gave them fraudulent information that it resulted from identity theft. The creditors may not then turn the fraudulent debts over to debt collectors.
- Dispute fraudulent or inaccurate information on your credit report with a credit reporting company. The credit reporting company must investigate your charges, and fix your report if they find that the information is fraudulent.

In many states, you have the right to restrict access to your credit report through a credit freeze. A credit freeze makes it more difficult for an identity thief to open a new account in your name. Your state attorney general's office has information about using a credit freeze where you live.

Dealing with Creditors, Debt Collectors, and Merchants

You have the right to:

- Have a credit report free of fraudulent accounts. Once you give creditors and debt collectors a copy of a valid identity theft report, they may not report fraudulent accounts to the credit reporting companies.
- Get copies of documents related to the theft of your identity — for example, applications used to open new accounts or transaction records — if you give the company a valid police report. You also can tell the company to give the documents to a specific law enforcement agency; that agency doesn't have to get a subpoena for the records.
- Stop the collection of fraudulent debts. You may ask debt collectors to stop contacting you to collect on fraudulent debts. You also may ask them to give you information related to the debt, like the names of the creditors and the amounts of the debts.

In many states, you have the right to be notified by a business or organization that has lost or misplaced certain types of personal information. Contact your state attorney general's office for more information.

Limiting Your Loss from Identity Theft

Various laws limit your liability for fraudulent debts caused by identity theft.

- **Fraudulent Credit Card Charges**: You cannot be held liable for more than $50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say cardholders who are victims of fraudulent transactions on their accounts have no liability for them at all.

- **Lost or Stolen ATM/Debit Card**: If your ATM or debit card is lost or stolen, you may not be held liable for more than $50 for the misuse of your card, as long as you

notify the bank or credit union within two business days after you realize the card is missing. If you do not report the loss of your card promptly, your liability may increase.

- **Fraudulent Electronic Withdrawals**: If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or debit card has not been lost or stolen, you are not liable, as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.

- **Fraudulent Checks**: Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact your state banking or consumer protection agency for more information.

- **Fraudulent New Accounts**: Under most state laws, you are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission. Contact your state attorney general's office for more information.

Other Federal Rights

Identity theft victims have other rights when the identity thief is being prosecuted in federal court. For example, under the Justice for All Act, the U.S. Department of Justice says identity theft victims have the right:

- to be reasonably protected from the accused;
- to reasonable, accurate, and timely notice of any public court proceeding, any parole proceeding involving the crime, or any release or escape of the accused;
- to not be excluded from any such public court proceeding unless the court determines that the identity theft victim's testimony would be materially altered if he or she heard other testimony at that proceeding;
- to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding;
- to confer with the attorney for the government in the case;
- to full and timely restitution as provided in law;
- to proceedings free from unreasonable delay; and
- to be treated with fairness and with respect for his or her dignity and privacy.

Other State Rights

You may have additional rights under state laws. Contact your state attorney general's office to learn more.

Average time to complete: 10 minutes

Identity Theft Victims' Complaint and Affidavit

A voluntary form for filing a report with law enforcement and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (___)_____
My evening phone: (___)_____
My email: _____

This section is for the victim's information, even if he or she cannot complete the form.

Leave (3) blank until you provide this form to someone with a legitimate business need, such as when you are filing your report at the police station or sending the form to a consumer reporting company to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (___)_____ My evening phone: (___)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

About the Fraud

What & When

(11) My personal information or documents (for example, credit cards, birth certificate, driver's license, Social Security card, etc.) were *lost or stolen* on or about _____.
mm/dd/yyyy

(12) I ***discovered*** that my personal information had been *used* by someone else on or about _____.
mm/dd/yyyy

(12): Let us know the date you ***noticed*** – this may be some time after the thief began to use it.

(13) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

(14) I ☐ did OR ☐ did not receive any money, goods, services, or other benefit as a result of the events described in this report.

Who

(15) I believe the following person(s) used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(15): Enter what you know (even if you can't complete everything) about anyone you believe was involved.

(A) Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (___)_____ (___)_____

Additional information about this person: _____

(B) Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(B) and (17): Attach additional sheets as needed.

Phone Numbers: (___)_____ (___)_____

Additional information about this person: _____

(16) I ☐ am OR ☐ am not willing to press charges and/or work with law enforcement if charges are brought against the person(s) who committed the fraud.

(17) Additional information (for example, how the identity thief gained access to your information or which documents or information were used):

About the Information or Accounts

(18) I wish to dispute the following personal information (such as my name, address, Social Security number, or date of birth) in my credit report as inaccurate as a result of this identity theft:

(A) _____
(B) _____
(C) _____

(19) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____
Company Name: _____
Company Name: _____

(20) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

(20):
If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Documentation

(21) I can verify my identity with these documents:

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport). *If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.*

☐ Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

Take these documents and this form to your local law enforcement office, along with your FTC complaint number (if you already filed online or by phone with the FTC). Ask an officer to witness your signature, below, and to complete the rest of the information about his or her department and your law enforcement report. It's important to get your report number, whether or not you are able to file in person.

Signature

If possible, sign and date *IN THE PRESENCE OF* a law enforcement officer.

(22) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains will be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Law Enforcement Report

(23) Select ONE:

☐ I was unable to file any law enforcement report.

☐ I filed an automated report with the law enforcement agency listed below.

☐ I filed my report in person with the law enforcement officer and agency listed below.

_____ _____

Law Enforcement Department State Report Number Filing Date (mm/dd/yyyy)

_____ _____

Officer's Name (please print) Officer's Signature Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

REMINDER: Attach copies of your identity documentation when sending your report to creditors and credit reporting agencies.

MODEL LETTER FOR THE COMPROMISE OF SOCIAL SECURITY NUMBERS

Dear _____:

We are contacting you about a potential problem involving identity theft.
[Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]

Your Name

FEDERAL TRADE COMMISSION | ftc.gov
1-877-FTC-HELP | FOR THE CONSUMER

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

June 2004

(610) Functionality in Emergency Situations

Carrier is able to remain functional in an emergency situation through the use of back-up power to ensure functionality without an external power source. Carrier has backup battery reserve in its central office, which enables it to provide service for a minimum of eight (8) hours. Carrier's service is consistent with the prior obligations to provide service in emergency situations as set forth in §54.202(a)(2) and Rule 46 of the Michigan Public Service Commission's Service Quality Rules (2000 AC, R 484.546), and its network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier has redundancy in its network for use for use in re-routing traffic when facilities are damaged.

(1010) Descriptive document for Voice Services Rate Comparability

We certify that Westphalia Telephone's rate of $22.82 is not greater than two standard deviations above the national average urban rate for voice service ($47.48).

Westphalia Telephone Company (310735)
Line 3010 – Milestone Certification

General Broadband Requirements

Westphalia Telephone Company (WTC) currently offers broadband service available at rates "reasonably comparable" to offerings of comparable broadband service in urban areas (Par. 91). For example, WTC currently offers 5 mbps downstream with a 1 mbps upstream for $34.95 per month. In the nearest urban area, Lansing Michigan, AT&T offers 6 mbps downstream with no advertised mbps upstream service for $34.95 per month.

Broadband Technical Requirements

WTC has tested their broadband service and determined that the following technical performance characteristics have been measured:

- Minimum actual speeds of 4 mbps downstream and 1 mbps upstream have been achieved at all reasonably feasible customer locations. Actual speed was measured from the end-user interface to the nearest internet access point.
- The time it takes for a packet of data to travel from one point in network to another has been tested to be less than 100 milliseconds. Actual latency was measured from the end-user interface to the nearest internet access point. This latency is suitable for real-time applications, including Voice over Internet Protocol.
- WTC currently has a data usage limit of 250 gigabytes per broadband customer per month; however, this usage limit has never been enforced. WTC does not have the equipment to monitor and impose data usage limits and it does not have any plans to buy any such equipment in the foreseeable future.

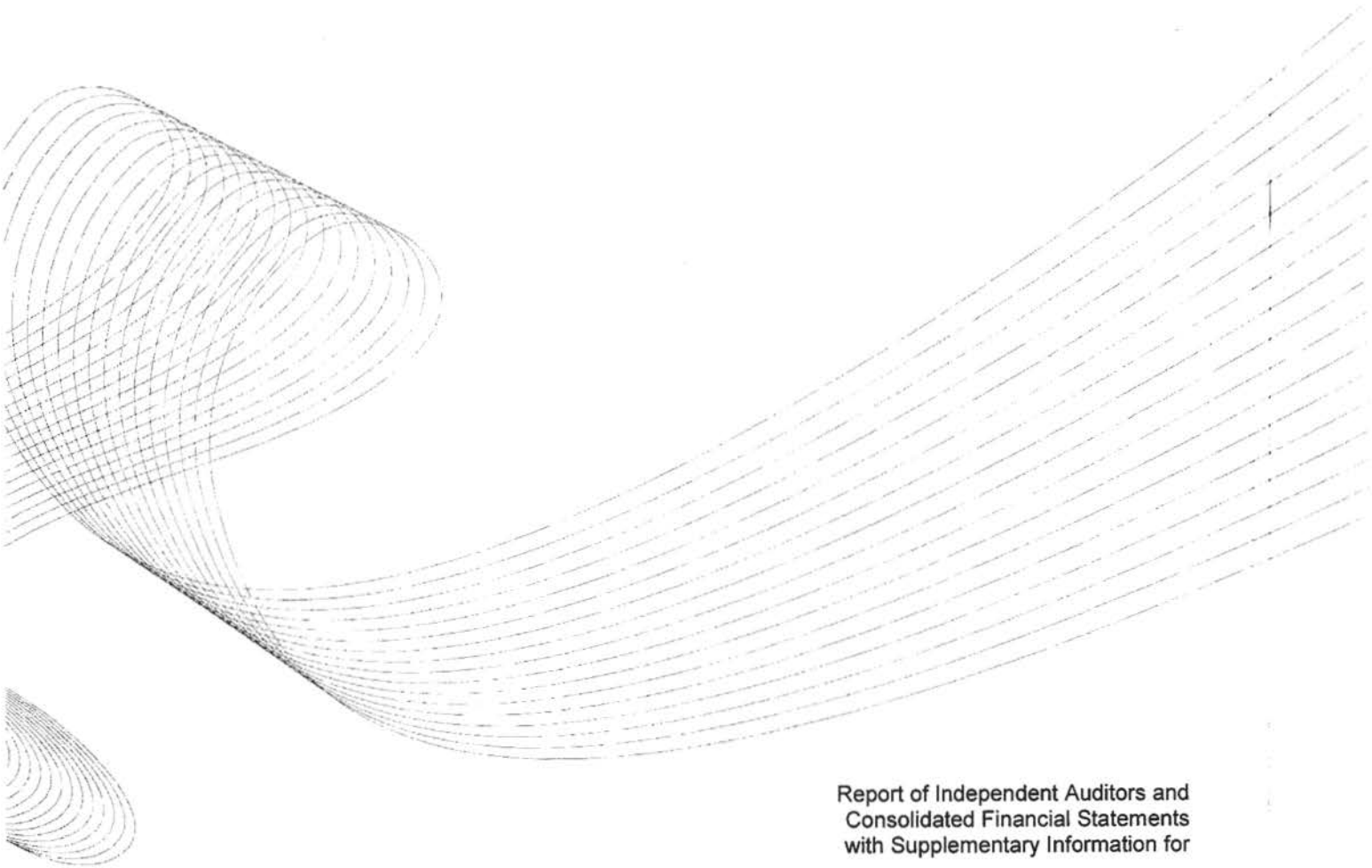
Broadband Build-Out Obligations

Upon receipt of a "reasonable request" for service, WTC will deploy services to the requesting customer within a "reasonable time". WTC's goal is to deploy services to a requesting customer in less than a week when it is reasonable. WTC currently deploys "scalable broadband" to their community. Facilities are not always built to meet a single customer request; rather, construction is on a scale which assumes service will be provided ultimately to a broader area surrounding that customer's location.

WTC will continue to assess requests for service for reasonableness and deploy the network in a scalable manner.

Westphalia Telephone Company was not provided a management letter for either their 2014 or 2013 audited financial statements. Located on pages 26 and 27 of this PDF file are the pages from the exit memo from our external auditors for the 2014 audited financial statements that is the communication with those charges with governance. Located on page 52 of this PDF file is the page from the exit memo from our external auditors for the 2013 audited financial statements that is the communication with those charges with governance. The exit memos are addressed to Great Lakes Comnet. Westphalia Telephone Company is a subsidiary of Clinton County Telephone Company and Clinton County Telephone Company is a subsidiary of Great Lakes Comnet. As such, Westphalia Telephone Company is covered by the Great Lakes Comnet exit memo.

Sincerely,
David Meyer
Accounting Manager
Westphalia Telephone Company
(517) 664-1900
dmeyer@comlink.net



Report of Independent Auditors and
Consolidated Financial Statements
with Supplementary Information for

Clinton County Telephone Company and Subsidiaries

December 31, 2014 and 2013

MOSS-ADAMS LLP

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.

CONTENTS